Ivanti Neurons for Secure Access

Des bases sécurisées pour l'Everywhere Workplace

Ivanti® Neurons for Secure Access permet aux entreprises de moderniser leurs déploiements VPN en regroupant Ivanti Connect Secure (VPN) et la gestion des accès Ivanti Neurons for Zero Trust Access. Cette nouvelle approche de gestion dans le Cloud permet, plus que jamais, de mieux contrôler et connaître le réseau et les accès.

Pour des bases d'accès sécurisé (Secure Access), partout

Gestion en continu des stratégies et des environnements pour autoriser l'accès aux applications et aux réseaux.

- Utilisation d'une approche de gestion dans le Cloud
- Prise en charge d'un modèle d'IT hybride (sur site, Cloud et périphérie)
- Compatible avec les systèmes Ivanti CS (VPN) anciens et nouveaux, et avec les environnements Ivanti Neurons for ZTA

Secure Access (accès sécurisé) applique une approche unique

Conception et personnalisation de votre parcours vers le SASE*

Nous sommes le seul fournisseur qui offre à la fois la possibilité de moderniser un déploiement VPN et celle de le transformer en architecture Zero Trust.

- Intégration facile des outils de VPN existants et déjà configurés
- Évolution vers le Zero Trust (c'est même le parcours le plus facile)
- Exploitation de l'un des atouts principaux d'Ivanti : l'architecture SDP (Périmètre défini par logiciel)

Gestion Secure Access, AUCUN changement de configuration nécessaire

Gestion plus fluide

Automatisation et meilleure gestion = sécurité renforcée et gain de temps pour l'équipe SecOps

- Apprentissage à partir du comportement des utilisateurs pour adapter la réponse de sécurité initiale, puis « à la volée »
- Utilisation d'une vue d'ensemble unique pour tous les utilisateurs, passerelles, périphériques et activités
- Allégement des efforts de gestion

Secure Access vous apporte un gain de temps pour les tâches de gestion entre 5 et 20 fois plus important.

(**par rapport aux outils de gestion VPN précédents)

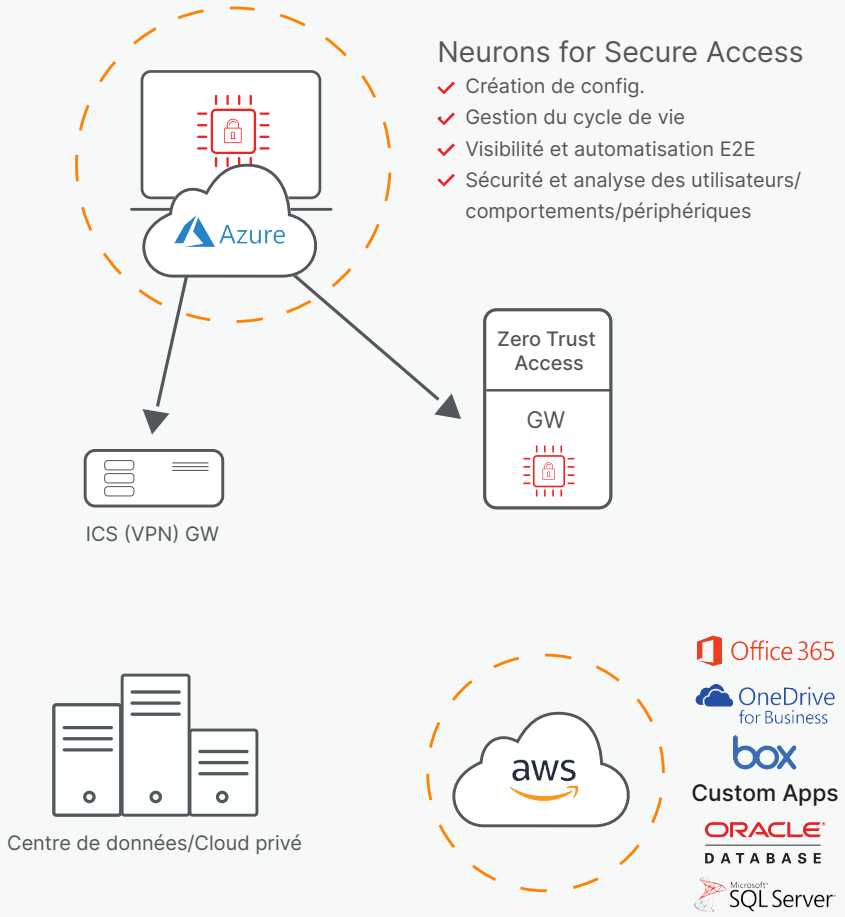
Comment ça marche

Neurons for Secure Access (nSA) est une plateforme de gestion centralisée et de reporting en SaaS, conçue pour fonctionner à la fois avec Ivanti Connect Secure et Ivanti Neurons for Zero Trust Access. Il fournit une interface unifiée qui permet aux responsables de sécurité de gérer plusieurs passerelles et/ou sites rapidement et efficacement.

nSA simplifie les workflows, car il regroupe toutes les données de journalisation, de reporting et d'activité dans une vue d'ensemble unique. Il fournit aussi aux administrateurs de puissants outils d'analyse pour examiner l'état de santé de leurs déploiements au quotidien. Des scores de risque propriétaires identifient les activités utilisateur non conformes ou anormales, ce qui permet aux administrateurs d'identifier les activités dangereuses et de réagir en conséquence. Grâce aux outils de planification de rapports, les administrateurs peuvent préparer, personnaliser et planifier des rapports contenant exactement les données qu'il leur faut, livrés directement dans leur boîte de réception.

nSA fonctionne avec les déploiements Ivanti Connect Secure (ICS) existants, et vous n'avez besoin ni d'implémenter du matériel supplémentaire, ni de modifier le réseau ou les connexions pour intégrer nSA dans un déploiement ICS. L'inscription d'une passerelle ICS auprès de nSA est très simple : vous lancez l'inscription dans nSA, puis l'achevez dans la passerelle. Le système établit alors des communications Websocket Secure entre la passerelle ICS et nSA. Une fois connectée, les journaux et analyses de la passerelle ICS sont téléchargés vers nSA. Vous pouvez les consulter ou générer des rapports à leur sujet dans le portail nSA. Les opérations de gestion des passerelles (permettant la mise à niveau, l'annulation (rollback) et le redémarrage, et fournissant des outils de dépannage) sont toutes activées une fois qu'ICS est connecté à nSA.

Neurons for Secure Access in Action



Fonction	Avantage
Bases Secure Access	■ Gère tous les aspects des passerelles Connect Secure et/ou des passerelles Zero Trust Access. ■ Prend en charge à la fois les passerelles VPN existantes et celles nouvelle génération. ■ Peut coexister avec des produits de VPN tiers
Gestion du cycle de vie des passerelles	■ Permet des mises à niveau, des rétrogradations et des redémarrages centralisés.
Gestion des configurations	■ Prise en charge des configurations de passerelle ■ Groupes de configuration pour une gestion des configurations sur plusieurs nœuds
Extensible, grâce à l'intégration d'outils tiers	■ Des API facilitent l'intégration facile d'autres outils (IDP, SIEM, UEM, évaluation des vulnérabilités et protection du poste client) ■ API REST
Visibilité, avec une seule « façade »	■ Visibilité globale et rapports de conformité des utilisateurs, des périphériques, des applications et de l'infrastructure pour toute l'entreprise.
Analyse du comportement des utilisateurs	■ Exploitez les données d'analyse pour limiter les risques de sécurité, détecter les anomalies, optimiser l'expérience utilisateur et vous adapter aux collaborateurs mobiles.
Débogage local (passerelle) et centralisé	■ Rétablissez plus rapidement le fonctionnement normal
Prise en charge des configurations hybrides	■ Possibilité de déployer les passerelles dans diverses configurations, y compris le Cloud

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com